The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue04 2025
PAGE NO. 1-5

The risks of cryptocurrencies to U.S. national security

Algirdas Degutis
Criminal Justice Research Department, Law Institute at Lithuanian Centre for Social Sciences, Vilnius, Lithuania

Received: 03 February 2025; **Accepted:** 02 March 2025; **Published:** 01 April 2025

Abstract: Cryptocurrencies have gained significant popularity over the past decade, attracting both legitimate users and illicit actors. While they offer a decentralized and secure method of transaction, the anonymous nature of cryptocurrencies presents serious threats to U.S. national security interests. This paper examines how cryptocurrencies are being used by malicious actors for activities such as money laundering, terrorism financing, and cyber-attacks. Additionally, it explores the challenges faced by U.S. Homeland Security in addressing these threats, and the implications for national security, law enforcement, and financial stability. The paper concludes with recommendations for strengthening U.S. regulatory frameworks and improving international cooperation to mitigate these risks.

Keywords: Cryptocurrencies, Homeland Security, National Security, Terrorism Financing, Money Laundering, Cybersecurity, U.S. Government, Regulatory Challenges.

Introduction: Cryptocurrencies, which are digital or virtual currencies that use cryptography for security, have gained significant traction over the past decade. Initially, they were designed to operate as decentralized alternatives to traditional fiat currencies, with Bitcoin being the first and most prominent example. However, the rise of cryptocurrencies has introduced a new set of challenges for national security agencies, particularly within the context of U.S. Homeland Security. While cryptocurrencies present opportunities for financial inclusion, lower transaction fees, and increased privacy for users, their pseudonymous nature and decentralized framework make them an appealing tool for illicit activities.

The decentralized characteristic of cryptocurrencies means that no central authority, such as a government or financial institution, controls them. This is a key feature that attracts both legitimate users and criminals alike. For legitimate users, cryptocurrencies offer greater autonomy over personal finances, secure transactions, and protection from currency devaluation. However, this same decentralization makes it difficult for authorities to regulate and track transactions, opening up avenues for exploitation by malicious actors. Terrorist organizations, criminal syndicates, and even rogue state actors have increasingly turned to cryptocurrencies to conduct illicit activities, bypassing traditional financial systems that are monitored by government agencies.

Cryptocurrencies provide a convenient platform for terrorism financing, money laundering, and cybercrimes such as ransomware attacks. These activities directly challenge U.S. national security interests, as they complicate law enforcement efforts and hinder the tracking of illicit financial flows. Terrorist organizations can use cryptocurrencies to raise and transfer funds anonymously, avoiding the scrutiny of financial institutions that would normally flag suspicious transactions. Likewise, criminal networks employ digital currencies to launder money, making it harder for authorities to trace the origins of illicit funds. In addition, the rise of cybercrime in the form of ransomware attacks has been largely fueled by cryptocurrencies, as victims are often required to pay ransoms in digital currencies, making it difficult for authorities to track down perpetrators.

The U.S. government has recognized these threats and has begun taking steps to address them, such as implementing regulations to monitor cryptocurrency exchanges and reporting requirements for digital asset transactions. However, the fast-evolving nature of cryptocurrency technology and the international aspect of many cryptocurrency-related crimes pose significant challenges to effective regulation and

enforcement. Cryptocurrencies can be easily transferred across borders, complicating efforts to track illegal activities and cooperate with foreign governments.

In this paper, we will explore the growing role of cryptocurrencies as a threat to U.S. homeland security interests. Specifically, we will examine how cryptocurrencies are exploited for terrorism financing, money laundering, and cybercrime, and analyze the regulatory challenges faced by U.S. authorities in combating these threats. Understanding these risks and the limitations of current regulatory measures is essential for improving U.S. security policies and preventing the exploitation of digital currencies by malicious actors.

Cryptocurrencies, digital assets built on decentralized blockchain technology, have revolutionized the way financial transactions are conducted. With Bitcoin's creation in 2009, cryptocurrencies have become an increasingly popular alternative to traditional financial systems, providing benefits such as lower transaction costs and increased privacy. However, this decentralization, coupled with the pseudonymous nature of blockchain transactions, poses a significant challenge for national security agencies, including U.S. Homeland Security. Cryptocurrencies are increasingly being used for illicit activities such as terrorism financing, money laundering, and ransomware attacks, creating new risks for U.S. national security.

The anonymity and cross-border nature of cryptocurrencies make it difficult for law enforcement to trace and prevent these activities. As such, cryptocurrencies present a significant threat to U.S. homeland security interests, and it is imperative to understand how these digital currencies are being exploited by malicious actors and the measures that need to be taken to address these threats.

METHODS

This paper adopts a qualitative research approach to examine the growing threat posed by cryptocurrencies to U.S. Homeland Security interests. The research methodology centers around a comprehensive review of existing literature, government reports, case studies, and relevant legal frameworks to understand how cryptocurrencies are used by illicit actors and the challenges faced by U.S. authorities in combating these threats.

The following steps were taken to conduct the research:

1. Literature Review and Data Collection The first step in the research process was to conduct an extensive literature review of peer-reviewed academic articles, government publications, and policy reports from organizations such as the U.S. Department of Homeland Security, the Financial Crimes Enforcement Network (FinCEN), and the U.S. Department of the Treasury. These documents were analyzed to understand how cryptocurrencies are utilized by criminal organizations, terrorist groups, and cybercriminals.

Key sources include:

o U.S. Government Reports: Documents issued by the U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and the Department of Homeland Security provided insights into how cryptocurrencies are used in the commission of crimes. Reports from the U.S. Treasury's Office of Terrorist Financing and Financial Crimes also offered valuable data on how digital currencies are employed to circumvent traditional financial oversight.

o Case Studies: Specific case studies, such as those involving ransomware attacks or instances of cryptocurrency being used to fund terrorism, were reviewed to understand the operational tactics employed by malicious actors. These real-world examples helped to contextualize the theoretical understanding of cryptocurrency threats within actual security incidents.

o Academic Journals and Research Papers: Research articles that focused on the intersection of technology, finance, and security were analyzed to gain a deeper understanding of the challenges in regulating cryptocurrencies. These included studies on the pseudonymity and encryption features of digital currencies, as well as blockchain's role in obfuscating illicit transactions.

2. Legal and Regulatory Analysis A significant portion of the research focused on analyzing the legal and regulatory frameworks established by U.S. authorities to monitor and control the use of cryptocurrencies. Key regulatory bodies, such as the Securities and Exchange Commission (SEC) and FinCEN, have issued guidelines aimed at curbing the misuse of cryptocurrencies for illegal purposes. The research examined these regulations to evaluate their effectiveness and the challenges they present in enforcement.

Key points of focus included:

o Anti-Money Laundering (AML) Regulations: FinCEN's regulatory framework for virtual currencies, which aims to treat cryptocurrency exchanges similarly to traditional financial institutions, was scrutinized to assess its impact on preventing money laundering and financing for illicit activities.

o Know Your Customer (KYC) Requirements: Analyzing the effectiveness of KYC regulations and their implementation at cryptocurrency exchanges, focusing on their ability to prevent the anonymity that terrorists and criminals seek when transacting in digital currencies.

o The Bank Secrecy Act (BSA): Understanding the BSA's influence on cryptocurrency transactions, and how this law is enforced by the U.S. government in its efforts to track financial activities related to terrorism and organized crime.

o International Regulatory Frameworks: The paper also examined how international regulations, such as those introduced by the Financial Action Task Force (FATF), interact with U.S. regulations. Given that cryptocurrencies are inherently global, understanding the international regulatory landscape was crucial for identifying gaps in cross-border enforcement.

3. Data Analysis of Cryptocurrency Transactions To gain a deeper understanding of the patterns and methods employed by illicit actors in the use of cryptocurrencies, the study examined various publicly available blockchain data analytics tools. These tools, such as Chainalysis and Elliptic, allow for the analysis of cryptocurrency transactions by mapping wallet addresses to known entities (such as exchanges or criminal groups). This type of blockchain forensic analysis enabled the research to identify trends in how cryptocurrencies are used to obscure the flow of illicit funds.

Specific areas of focus in this analysis included:

o Identifying Red Flags in Cryptocurrency Transactions: By analyzing transactions associated with known ransomware attacks, terrorist organizations, and illicit money laundering schemes, the study aimed to identify common patterns and red flags that indicate misuse of cryptocurrencies.

o Mapping Terrorist Financing: Case studies such as those involving the use of Bitcoin by organizations like ISIS and Al-Qaeda were analyzed to see how they exploited cryptocurrency's pseudonymous nature to raise funds through online campaigns and donations.

o Tracking Ransomware Payments: Cryptocurrency's use in ransomware payments was explored by looking at the specific digital wallets and addresses associated with known cybercrime groups. This analysis highlighted the difficulties faced by authorities in tracing payments and identifying perpetrators.

4. Interviews with Experts While the primary research was conducted using secondary sources, interviews with subject-matter experts in the fields of cybersecurity, financial crime investigation, and cryptocurrency regulation were conducted to gain insights into the challenges and opportunities in addressing the use of digital currencies for illicit purposes. Experts from federal agencies, private sector security firms, and financial institutions were consulted to provide a holistic understanding of the practical challenges faced by U.S. authorities. These interviews were semi-structured and provided a platform for expert opinions on potential solutions, as well as gaps in the current regulatory frameworks.

5. Comparative Analysis of Global Responses Finally, the paper compared the U.S. response to cryptocurrency-related threats with those of other countries and international organizations. This comparative analysis aimed to identify best practices and lessons learned from jurisdictions that have implemented successful regulatory frameworks to combat cryptocurrency misuse. Countries such as China, South Korea, and the European Union were studied to assess how they are tackling cryptocurrency-related threats through regulations, law enforcement coordination, and technological innovation. The international response was also examined to assess the effectiveness of cross-border cooperation in tracking and combating cryptocurrency-based crimes.

The combination of these research methods allowed for a comprehensive understanding of the multifaceted ways in which cryptocurrencies threaten U.S. Homeland Security interests. The analysis not only provided a clearer picture of how cryptocurrencies are being used for illicit activities but also highlighted the regulatory gaps and enforcement challenges faced by U.S. authorities. The results of this research are intended to inform future policy recommendations aimed at mitigating the risks posed by cryptocurrencies to U.S. national security.

This paper employs a qualitative research approach, analyzing existing literature, reports, and case studies from sources such as government agencies, academic journals, and financial regulatory bodies. A critical examination of the role of cryptocurrencies in illegal activities was conducted by reviewing publicly available data on terrorist organizations, cybercriminals, and money laundering networks that utilize digital currencies. Additionally, legal and regulatory frameworks developed by the U.S. government and international organizations were analyzed to assess their effectiveness in combating the illicit use of cryptocurrencies.

RESULTS

The findings from the analysis indicate that cryptocurrencies are increasingly being used in a

variety of ways that pose a direct threat to U.S. Homeland Security interests:

1. Terrorism Financing: Cryptocurrencies provide terrorist organizations with a method of transferring funds across borders without the oversight of traditional financial institutions. The pseudonymous nature of blockchain transactions makes it difficult for authorities to trace these funds back to their sources or intended recipients. Groups such as ISIS and Al-Qaeda have reportedly used cryptocurrencies for fundraising and operational support.

2. Money Laundering: Criminal organizations exploit cryptocurrencies to launder illicit funds. Cryptocurrencies provide a way to obscure the origin of illicit assets, enabling criminals to move money across jurisdictions without detection. This creates challenges for anti-money laundering (AML) regulations and enforcement.

3. Cybersecurity Threats: Cybercriminals use cryptocurrencies to demand ransom from victims of cyber-attacks, particularly ransomware incidents. These attacks have targeted critical U.S. infrastructure, including government entities, healthcare institutions, and private corporations. The use of cryptocurrencies for ransom payments makes it harder for authorities to track and apprehend perpetrators.

4. Regulatory Challenges: Current U.S. regulatory frameworks are insufficient to fully address the rapidly evolving landscape of cryptocurrency-related threats. While agencies such as the Financial Crimes Enforcement Network (FinCEN) have made strides in regulating cryptocurrency exchanges and users, gaps in enforcement and international cooperation persist.

DISCUSSION

Cryptocurrencies are undeniably a powerful tool for enabling decentralized financial transactions; however, their misuse by criminal and terrorist actors poses a significant challenge for U.S. Homeland Security. The key threat lies in the lack of centralized control over digital currencies, which makes enforcement of existing laws and regulations more complicated. Criminals and terrorists can exploit cryptocurrencies to bypass the traditional financial system, making it difficult for U.S. authorities to trace illicit financial flows and enforce counterterrorism and anti-money laundering measures.

The decentralized nature of cryptocurrencies also complicates global cooperation on law enforcement. While some countries have developed regulatory frameworks to combat cryptocurrency-based crimes, there is no universal standard for cryptocurrency regulation, and enforcement varies significantly across jurisdictions. This fragmentation undermines the ability of the U.S. to collaborate with international partners and address cross-border criminal activity effectively.

In addition, the rapid evolution of blockchain technology and cryptocurrency applications, such as decentralized finance (DeFi) and non-fungible tokens (NFTs), adds new layers of complexity to the situation. As these technologies grow, the potential for their exploitation by malicious actors increases, requiring a proactive and adaptive approach by U.S. Homeland Security.

CONCLUSION

Cryptocurrencies present a growing threat to U.S. Homeland Security interests due to their misuse in financing terrorism, laundering money, and facilitating cybercrime. To effectively mitigate these risks, the U.S. must enhance its regulatory frameworks, improve collaboration between federal, state, and international law enforcement agencies, and stay ahead of technological advancements. Strengthening anti-money laundering (AML) regulations, improving cryptocurrency exchange monitoring, and fostering international cooperation are essential steps to combating the illicit use of cryptocurrencies. Failure to address these threats could result in increased vulnerabilities to national security, economic stability, and public safety.

REFERENCES

Alasmari, Khaled A. A. 2012. Cleaning up Dirty Money: The Illegal Narcotics Trade and Money Laundering. Economics & Sociology 5: 139–48. [Google Scholar]

Becker, Jasper. 2005. Rogue Regime: Kim Jong Il and the Looming Threat of North Korea. Oxford: Oxford University Press. [Google Scholar]

Biden, Joseph Robinette. 2021. Executive order on Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade. December 15. Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/15/executive-order-on-imposing-sanctions-on-foreign-persons-involved-in-the-global-illicit-drug-trade/ (accessed on 29 July 2024).

Busch, Nathan E., and Austen D. Givens. 2014. The Business of Counterterrorism: Public-Private Partnerships in Homeland Security. New York: Peter Lang. [Google Scholar]

Clunan, Anne. 2006. The Fight against Terrorist Financing. Political Science Quarterly 121: 569–96. [Google Scholar] [CrossRef]

Council on Foreign Relations. 2022. What to Know About Sanctions on North Korea. July 27. Available online: https://www.cfr.org/backgrounder/north-

korea-sanctions-un-nuclear-weapons (accessed on 27 December 2024).

Crandall, Russell. 2020. Drugs and Thugs: The History and Future of America's War on Drugs. New Haven: Yale University Press. [Google Scholar]

DeFeo, Michael A. 1990. Depriving International Narcotics Traffickers and Other Organized Criminals of Illegal Proceeds and Combatting Money Laundering. Denver Journal of International Law & Policy 18: 405–15. [Google Scholar]

Department of Homeland Security. 2022a. Human Trafficking Laws & Regulations. November 9. Available online: https://www.dhs.gov/human-trafficking-laws-regulations (accessed on 29 July 2024).

Department of Homeland Security. 2022b. What Is Human Trafficking? September 22. Available online: https://www.dhs.gov/blue-campaign/what-human-trafficking (accessed on 29 July 2024).

Department of Homeland Security. 2023. Counter Terrorism and Homeland Security Threats. May 30. Available online: https://www.dhs.gov/counter-terrorism-and-homeland-security-threats (accessed on 29 July 2024).

Department of Homeland Security. 2024. DHS Center for Countering Human Trafficking. July 2. Available online: https://www.dhs.gov/dhs-center-countering-human-trafficking (accessed on 29 July 2024).

Department of Justice. 2020a. Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Available online: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (accessed on 29 July 2024).

Department of Justice. 2020b. Report of the Attorney General's Cyber Digital Task Force. October. Available online: https://www.justice.gov/d9/pages/attachments/2021/01/20/cryptocurrency_white_paper.final_.pdf (accessed on 29 July 2024).

Department of Justice. 2022. Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace. April 5. Available online: https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (accessed on 29 July 2024).

Department of State. 2020. Country Reports on Terrorism 2020: Iran. Available online: https://www.state.gov/reports/country-reports-on-terrorism-2020/iran (accessed on 14 October 2024).

Department of State. n.d. Foreign Terrorist Organizations. Available online: https://www.state.gov/foreign-terrorist-organizations/ (accessed on 29 July 2024).

Department of the Treasury. 2020. Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity. October 15. Available online: https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf (accessed on 29 July 2024).

Devon, Cheyenne. 2023. A Crypto Exchange Allegedly Processed over $700 Million Worth of Illicit Funds Before the Department of Justice Shut it Down. CNBC.com. January 20. Available online: https://www.cnbc.com/2023/01/20/justice-dept-shuts-down-crypto-exchange-that-processed-illicit-funds.html (accessed on 29 July 2024).

Dwyer, Gerald P. 2015. The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability 17: 81–91. [Google Scholar] [CrossRef]

Frebowitz, Ryan L. 2018. Cryptocurrency and State Sovereignty. Naval Postgraduate School. Available online: https://apps.dtic.mil/sti/pdfs/AD1059865.pdf (accessed on 16 July 2024).

Ganor, Boaz. 2002. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? Policy Practice and Research: An International Journal 3: 287–304. [Google Scholar] [CrossRef]

George, Derek R. 2018. Cryptocurrencies: Emergent Threat to National Security. Marine Corps University. Available online: https://apps.dtic.mil/sti/trecms/pdf/AD1179035.pdf (accessed on 16 July 2024).

Gholipour, Benham. 2021. Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions. March 2. Iranwire.com. Available online: https://iranwire.com/en/features/69084/ (accessed on 29 July 2024).

Giudici, Giancarlo, Alistair Milne, and Dmitri Vinogradov. 2020. Cryptocurrencies: Market analysis and perspectives. Journal of Industrial and Business Economics 47: 1–18. [Google Scholar] [CrossRef]

Givens, Austen D., Nathan E. Busch, and Alan D. Bersin. 2018. Going Global: The International Dimensions of U.S. Homeland Security Policy. Journal of Strategic Security 11: 1–34. [Google Scholar] [CrossRef]